

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

98 227 #^{KS}₂
1-549 U.S. PTO
09/488653
01/20/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

1999年 1月21日

願番号
Application Number:

平成11年特許願第013215号

願人
Applicant(s):

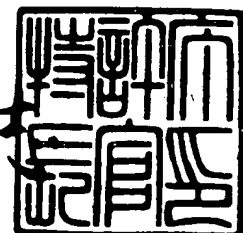
インターナショナル・ビジネス・マシーンズ・コーポレイシ
ョン

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年 5月14日

特許庁長官
Commissioner,
Patent Office

伴佐山 建



【書類名】 特許願

【整理番号】 JA998227

【あて先】 特許庁長官 殿

【国際特許分類】 G08B 13/00
G08B 13/24
G06F 1/00

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ビー・エム株式会社 大和事業所内

【氏名】 田 中 順

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ビー・エム株式会社 大和事業所内

【氏名】 堀 越 秀 人

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ビー・エム株式会社 大和事業所内

【氏名】 野 村 雅 彦

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ビー・エム株式会社 大和事業所内

【氏名】 臼 井 英 之

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ビー・エム株式会社 大和事業所内

【氏名】 堀 越 正 太

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ビー・エム株式会社 大和事業所内

【氏名】 田 村 文 雄

【特許出願人】

【識別番号】 390009531

【住所又は居所】 アメリカ合衆国 10504、ニューヨーク州アーモンク
(番地なし)

【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレ
イション

【代理人】

【識別番号】 100086243

【弁理士】

【氏名又は名称】 坂口 博

【連絡先】 0462-73-3318、3325、3455

【選任した代理人】

【識別番号】 100091568

【弁理士】

【氏名又は名称】 市位 嘉宏

【手数料の表示】

【予納台帳番号】 024154

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9304391

【包括委任状番号】 9304392

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティ機能付きコンピュータおよび方法

【特許請求の範囲】

【請求項 1】 コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

(a) 前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、

(b) 前記ステップ (a) のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、

(c) 前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、

(d) 前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、

(e) 前記ステップ (c) およびステップ (d) に応答して前記コンピュータへのアクセスを禁止するステップと
を有する方法。

【請求項 2】 前記ステップ (b) を、前記コンピュータのパワー・オン、省エネ・モードの変更、および特定のファイルへのアクセスからなるグループから選択された一つの要素に応答して開始する請求項 1 記載の方法。

【請求項 3】 前記ステップ (e) を適切なパスワードの入力がない場合にのみ実行する請求項 1 記載の方法。

【請求項 4】 コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

(a) 前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、

(b) 前記ステップ (a) のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、

(c) 前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、

(d) 前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、

(e) 前記ステップ(c)およびステップ(d)に応答して、装着されたことがある前記セキュリティ装置が現在脱着されていることを示すデータを前記第一の記憶手段の第二の記憶領域に記憶し保持するステップと、

(f) 前記ステップ(e)に応答して前記コンピュータへのアクセスを禁止するステップと
を有する方法。

【請求項5】コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

(a) 前記コンピュータに装着されたセキュリティ装置が脱着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第二の記憶領域に記憶するステップと、

(b) 前記ステップ(a)のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、

(c) 前記第二の記憶領域のデータに基づいて前記装着されたセキュリティ装置が脱着されたことを検出するステップと、

(d) 前記ステップ(c)に応答して前記コンピュータへのアクセスを禁止するステップと
を有する方法。

【請求項6】コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

(a) 前記コンピュータに前記セキュリティ装置が装着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、

(b) 前記コンピュータから前記セキュリティ装置が脱着されていないか否かを前記コンピュータに装備された演算処理装置が定期的に監視するステップと、

(c) 前記ステップ (b) に応答して前記コンピュータへのアクセスを禁止するステップと
を有する方法。

【請求項 7】セキュリティ装置の装着ができるコンピュータであって、
前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

(a) 前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、(b) 前記ステップ (a) のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、(c) 前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、(d) 前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、(e) 前記ステップ (c) およびステップ (d) に応答して前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶したコンピュータによる読みとりが可能な第二の記憶手段と
を有するコンピュータ。

【請求項 8】セキュリティ装置の装着ができるコンピュータであって、
前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

(a) 前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、(b) 前記ステップ (a) のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、(c) 前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、(d) 前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、(e) 前記ステップ (c) およ

びステップ（d）に回答して、装着されたことがある前記セキュリティ装置が現在脱着されていることを示すデータを前記第一の記憶手段の第二の記憶領域に記憶し保持するステップと、（f）前記ステップ（e）に回答して前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶したコンピュータによる読みとりが可能な第二の記憶手段とを有するコンピュータ。

【請求項 9】セキュリティ装置の装着ができるコンピュータであって、前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

（a）前記コンピュータに装着されたセキュリティ装置が脱着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第二の記憶領域に記憶するステップと、（b）前記ステップ（a）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、（c）前記第二の記憶領域のデータに基づいて前記装着されたセキュリティ装置が脱着されたことを検出するステップと、（d）前記ステップ（c）に回答して前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶したコンピュータによる読みとりが可能な第二の記憶手段とを有するコンピュータ。

【請求項 10】セキュリティ装置の装着ができるコンピュータであって、前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

（a）前記コンピュータに前記セキュリティ装置が装着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、（b）前記コンピュータから前記セキュリティ装置が脱着されたか否かを前記コンピュータに装備された演算処理装置が定期的に監視するステップと、（c）前記ステップ（b）に回答して前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶した

コンピュータによる読みとりが可能な第二の記憶手段と
を有するコンピュータ。

【請求項 11】セキュリティ装置の着脱ができるコンピュータであって、
前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶
手段と、

演算処理装置と、

前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記
第一の記憶手段の第一の記憶領域に記憶させる手段と、

前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ
装置が装着されたことがあることを検出する手段と、

前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出
する手段と、

前記検出手段に応答して前記コンピュータへのアクセスを禁止する手段と
を有するコンピュータ。

【請求項 12】セキュリティ装置の着脱ができるコンピュータであって、
前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶
手段と、

演算処理装置と、

前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記
第一の記憶手段の第一の記憶領域に記憶させる手段と、

前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ
装置が装着されたことがあることを検出する第一の検出手段と、

前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出
する第二の検出手段と、

前記第一および第二の検出手段に応答して、装着されたことがある前記セキュ
リティ装置が現在脱着されていることを示すデータを前記第一の記憶手段の第二
の記憶領域に記憶させる手段と、

前記第二の記憶領域に記憶されたデータに応答して前記コンピュータへのアク
セスを禁止する手段と

を有するコンピュータ。

【請求項 1 3】セキュリティ装置の装着ができるコンピュータであって、
前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

前記コンピュータに装着されたセキュリティ装置が脱着されたことを示すデータを前記第一の記憶手段の第二の記憶領域に記憶させる手段と、

前記第二の記憶領域のデータに基づいて前記装着されたセキュリティ装置が脱着されたことを検出する検出手段と、

前記検出手段に応答して前記コンピュータへのアクセスを禁止する手段と
を有するコンピュータ。

【請求項 1 4】セキュリティ装置の装着ができるコンピュータであって、
前記コンピュータの主電源が停止している状態で記憶保持が可能が第一の記憶手段と、

前記コンピュータに前記セキュリティ装置が装着されたことを示すデータを前記第一の記憶手段の第一の記憶領域に記憶させる手段と、

前記コンピュータから前記セキュリティ装置が脱着されたか否かを定期的に監視する演算処理装置と、

前記前記演算処理装置の監視結果に応答して前記コンピュータへのアクセスを禁止する手段と

を有するコンピュータ。

【請求項 1 5】前記第一の記憶手段が R F I D システムに使用する R F I D タグであり、前記セキュリティ装置が R F アンテナである請求項 7 ないし請求項 1 4 のいずれかに記載のコンピュータ。

【請求項 1 6】前記 R F アンテナが前記コンピュータのデバイス・ベイの蓋に装着されている請求項 7 ないし 1 4 のいずれかに記載のコンピュータ。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、コンピュータの盗難および不正アクセス等を防止するためにコンピュータ本体に取り外し可能に装着されたセキュリティ機能の一部を担う装置が不正に取り外された場合に、コンピュータへのアクセスを禁止する技術に関する。

【0002】

【従来の技術】

ノートブック型コンピュータは携帯性に優れている反面、きわめて容易に不正に外部に持ち出される。近年のコンピュータ利用の高度化および多様化に伴い、ユーザは貴重な情報をコンピュータ内部に格納する傾向がますます強まり、コンピュータが盗難に合うとその物理資源の損失に比べて情報資源の漏洩による損失が一層甚大になってきている。

【0003】

特開平8-50690号公報および特開平10-124764号公報は、RF（ラジオ周波数）トランスポンダ・システムという非接触的な通信技術を用いた電子式物品監視システムを開示する。RFトランスポンダ・システムは、一般的に励振器（Exicter）／読取器（Reader）すなわちER、およびRFIDトランスポンダあるいはRFID（Radio Frequency Identification）タグと呼ばれるものを含んでいる。監視区域内の物品にRFIDタグを取り付け、その領域の出入口にERを設置して常時RF励振信号を発生させる。出入口にRFIDタグが取り付けられた物品が接近するとERがこれに励振信号を送信して電力を与えるのでRFIDタグ自体は特に動作用の電力を必要としない。RF励振信号を受け取ったRFIDタグは識別コードその他のデータ信号を発生し、特定の周波数でERに応答信号として送り返す。この応答信号中に含まれる識別コードをERが検出すると必要に応じてアラーム音を発生して物品の盗難を防止する。物品を監視区域内からアラーム音を発生させないで持ち出すには、RFIDタグをアラーム信号を送信しない状態にセットするかこれを脱着する必要がある。

【0004】

特開平5-35354号公報は、ノートブック型コンピュータの盗難防止を図る技術を開示する。ノートブック型コンピュータに、設置傾斜量、設置圧力および設置距離等の設置状態の変化を検出する盗難防止手段と設置状態の変化に応答

して警報を発する手段を設ける。これらの手段が機能を発揮する状態にあるときコンピュータは設置状態を常時監視し、コンピュータを許可なく定位置から持ち運ぼうとした際に警報を発して盗難を防止する。

【0005】

特開平3-100894号公報は、携帯端末が盗難に合ったときにキー入力を停止して不正なアクセスを禁止する技術を開示する。携帯端末が盗難に合うと、ホストコンピュータから無線で端末に特定の信号を送り、それに応答して端末内部のプログラムが作動してキー入力ができない状態にする。

【0006】

【発明が解決しようとする課題】

上述したようにRFIDタグを使用して物品の盗難を防止する技術が知られており、またノートブック型コンピュータが監視区域から不正に持ち出されることを防止する技術およびコンピュータの盗難時にキー入力をロックして情報資源を保護する技術も知られている。しかし、RFIDタグをコンピュータに装着して盗難に合ったコンピュータへの不正アクセスを防止する技術は開示されていない。

【0007】

ところで、盗難防止または記憶情報への不正アクセスを防止するには、コンピュータにRFIDタグのような装置を装備する必要がある。一方このような装置は、すべてのユーザが必要とするものではなく、一般に企業内で大規模に使用している場合に比べて個人的範囲でのみ使用するユーザにとっては必要性が少ない。セキュリティ機能をすべてのコンピュータに装備して販売することは、必要のないユーザに対して余分な費用を強いることになり好ましくない。したがって、特定のシリーズに含まれる同一タイプのコンピュータにおいて、セキュリティ機能を装備するものとセキュリティ機能を装備しないものを用意する必要がある。

【0008】

ところで、特定のシリーズに含まれるコンピュータは、できるだけハードウェアおよびソフトウェアの共通化を図ることが販売コストおよび販売後のサービス

の維持という面で好ましい。特定のシリーズのコンピュータをセキュリティ機能を装備するものと装備しないものとに分けて製造および販売することは、一見セキュリティ機能を必要としないユーザの費用負担を公平にできるようにみえるが、共通化ができない部分での費用負担が増加し結果としてそのようなユーザにとっても不利になる。ここに、ハードウェアおよびソフトウェアの共通化とユーザによるセキュリティ機能の選択による費用負担の公平性という課題を同時に解決する必要が生じてくる。

【0009】

これを解決する方法として、あるセキュリティ機能が複数のハードウェアおよびソフトウェアの構成要素からなる場合にその構成要素のある部分までを共通にし、残りの一部を販売店またはユーザが必要に応じて追加できるオプション部品にしてセキュリティ機能を完成できるようにする方法がある。しかし、セキュリティ機能の一部を担う装置をユーザまたは販売店で装着するようにすると（このような装置を以後単にセキュリティ装置という。）、その部分が不正に脱着されてセキュリティ機能が毀損されてしまうことが予測される。

【0010】

したがって本発明の目的は、コンピュータのセキュリティ機能を担う一部の装置、すなわちセキュリティ装置がコンピュータから不正に脱着されたときに、コンピュータへのアクセスを禁止する技術を提供することにある。さらに本発明の目的は、セキュリティ機能を備えるコンピュータと備えないコンピュータとの間でセキュリティ装置のみをオプションとし、他のハードウェアおよびソフトウェアは両コンピュータに共通のものを組み込んだコンピュータを提供することにある。さらにまた本発明の目的は、ユーザまたは販売店がオプションに取り付けるセキュリティ装置の好適な取り付け構造を提供することにある。

【0011】

【課題を解決するための手段】

本発明に係るコンピュータはセキュリティ装置をオプションに取り付けることができる構造を備え、セキュリティ装置を装着することによりセキュリティ機能を具備したコンピュータを構成し、セキュリティ装置を脱着することでセキ

リティ機能を具備しないコンピュータを構成する。本発明においてコンピュータへのアクセスを禁止する手順は、コンピュータのパワー・オン、省エネ・モードの変更、特定のファイルへのアクセス等の特定のイベントに関連付けて開始させることができるが、常時CPUにポーリングにより監視させてもよい。特定のイベントに関連付けて開始させると、CPUの負担を軽くすることができる。

【0012】

本発明の一の態様では、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、(a) 前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、(b) 前記ステップ(a)のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、(c) 前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、(d) 前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、(e) 前記ステップ(c)およびステップ(d)に応答して前記コンピュータへのアクセスを禁止するステップとを備える。

【0013】

本発明においてセキュリティ装置とは、コンピュータのセキュリティ機能の一部を担うハードウェアであって、オプション部品として用意されユーザまたは販売店で脱着可能な程度の装着容易性を備える装置をいう。たとえばRFIDを利用したセキュリティ・システムではRFアンテナでもよく、指紋検出を利用したセキュリティ・システムでは指紋入力部であってもよい。第一の記憶手段はコンピュータの主電源が停止した状態で記憶内容を保持できる記憶媒体でEEPROMまたはハードディスク等を選定できる。さらに二次電池により主電源が停止している場合でも記憶保持ができる電力が供給され続けているRAMであってもよい。この手順はセキュリティ機能を備えるコンピュータおよび備えないコンピュータのいずれに対しても共通に実行でき、セキュリティ機能を備えるコンピュータについてのみセキュリティ装置が脱着されたときにアクセスが禁止される。

【0014】

上記第一の態様においては、ステップ（a）により、このコンピュータがセキュリティ機能を備えたコンピュータであることがシステムにより認識され、コンピュータからセキュリティ装置が脱着された場合は不正行為があったものとして以下の手順によりパスワードを入力しない限りコンピュータへのアクセスが禁止される。ステップ（b）によりコンピュータへのアクセスを禁止する手順がセキュリティ機能を備えるコンピュータにもセキュリティ機能を備えないコンピュータにも開始される。ステップ（c）により、このコンピュータがセキュリティ機能を備えるコンピュータであることが確認される。ステップ（d）によりコンピュータからセキュリティ装置が脱着されていることが確認され、これは不正行為としてステップ（e）でコンピュータへのアクセスが禁止される。適正にセキュリティ装置を脱着する場合は、パスワードを入れてアクセスを確保することができる。

【0 0 1 5】

本発明の第二の態様は、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、（a）前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、（b）前記ステップ（a）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、（c）前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、（d）前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、（e）前記ステップ（c）およびステップ（d）に応答して、装着されたことがある前記セキュリティ装置が現在脱着されていることを示すデータを前記第一の記憶手段の第二の記憶領域に記憶し保持するステップと、（f）前記ステップ（e）に応答して前記コンピュータへのアクセスを禁止するステップとを備える。

【0 0 1 6】

上記態様のステップ（e）では、一旦セキュリティ装置が装着されてこのコンピュータがセキュリティ機能を備えるコンピュータであることをシステムが認識

したのちにセキュリティ装置が取り外されたことがある場合は、そのコンピュータに対して不正なアクセスがあったことを示すデータとして記憶させる。このデータは、以後リセットされない限り第二の記憶領域に記憶保持される。

【 0 0 1 7 】

本発明の第三の態様では、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、（a）前記コンピュータに装着されたセキュリティ装置が脱着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第二の記憶領域に記憶するステップと、（b）前記ステップ（a）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、（c）前記第二の記憶領域のデータに基づいて前記装着されたセキュリティ装置が脱着されたことを検出するステップと、（d）前記ステップ（c）に応答して前記コンピュータへのアクセスを禁止するステップとを備える。

【 0 0 1 8 】

ステップ（a）のデータは、本発明の第二の態様で示した方法で記憶してもよい。ステップ（c）でこのデータを確認することにより、ステップ（b）で開始した手順の実行段階ではセキュリティ装置が装着されていたとしても、それ以前に少なくとも一度はセキュリティ装置が脱着されたことがあるのでコンピュータへのアクセスが禁止される。

【 0 0 1 9 】

本発明の第四の態様では、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、（a）前記コンピュータに前記セキュリティ装置が装着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、（b）前記コンピュータから前記セキュリティ装置が脱着されたか否かを前記コンピュータに装備された演算処理装置が定期的に監視するステップと、（c）前記ステップ（b）に応答して前記コンピュータへのアクセスを禁止するステップとを備える。

【 0 0 2 0 】

ステップ（b）では、セキュリティ機能を備えるコンピュータにおいて演算処理装置にセキュリティ装置が脱着されたことを定期的に監視させる。この場合はコンピュータの電源が入っていることが前提になるが、セキュリティ装置が脱着されたあとに演算処理装置の定期的な監視のタイミングでアクセスを禁止することができる。

【0021】

本発明の第一ないし第四の態様で説明した各ステップは、コンピュータ・プログラムによりコンピュータ上で実行させることができる。このようなプログラムは第二の記憶手段として利用できるEEPROMまたはFLASH ROMといわれる不揮発性のメモリや、ハードディスク、フロッピー・ディスク等に記憶させることができ、コンピュータの動作時にメイン・メモリに読み出して演算処理装置で実行させることができる。

【0022】

本発明のセキュリティ装置は、デバイス・ベイの蓋部に組み込むことで、コンピュータの余分なスペースを消費することなくオプション部品とすることができる。デバイス・ベイの蓋は、セキュリティ装置を組み込んだ蓋とセキュリティ装置を組み込んでいない単なる蓋の二つをオプション部品としていずれか一つを選択できるようにし、ユーザまたは販売店でコンピュータに装着できる。

【0023】

【発明の実施の形態】

〔コンピュータ・システムの概要〕

図1には、本発明を実施するのに適した典型的なノート型パーソナル・コンピュータ10のハードウェア構成をサブシステム毎に模式的に示している。CPU11は、OSの制御下で、各種プログラムを実行するようになっている。CPU11は、システム・バス13を経由して、一般にメモリ／PCI制御チップ15と呼ばれるブリッジ回路（ホスト－PCIブリッジ）に接続されている。本実施例のメモリ／PCI制御チップ15は、メイン・メモリ17へのアクセス動作を制御するためのメモリ・コントローラ機能や、システム・バス13とPCIバス19間のデータ転送速度の差を吸収するためのデータ・バッファなどを含んだ構

成となっている。

【0024】

メイン・メモリ 17 は、CPU 11 の実行プログラムの読み込み領域として、あるいは実行プログラムの処理データを書き込む作業領域として利用される、書き込み可能メモリである。ここで言う実行プログラムには、Windows 98 などの OS、周辺機器類をハードウェア操作するための各種デバイス・ドライバ、特定業務に向けられたアプリケーション・プログラムや、FLASH ROM 49 に格納された BIOS が含まれる。ビデオ・サブシステム 21 は、ビデオに関連する機能を実現するためのサブシステムであり、CPU 11 からの描画命令を実際に処理し、処理した描画情報をビデオ・メモリ (VRAM) に一旦書き込むとともに、VRAM から描画情報を読み出して液晶ディスプレイ (図示せず。) に描画データとして出力するビデオ・コントローラを含む。

【0025】

カードバス・コントローラ 23 は、PCI バス 19 のバス・シグナルを PCI カード・スロット 25 のインタフェース・コネクタ (カードバス) に直結させるための専用コントローラである。PCI バス 19 と I/O バス 39 とは、多機能 PCI デバイス 27 によって相互接続されている。本実施例の多機能 PCI デバイス 27 は、PCI バス 19 と I/O バス 39 とのブリッジ機能、DMA コントローラ機能、プログラマブル割り込みコントローラ (PIC) 機能、及びプログラマブル・インターバル・タイマ (PIT) 機能、IDE (Integrated Drive Electronics) インタフェース機能、USB (Universal Serial Bus) 機能、SMB (System Management Bus) インタフェース機能を備えており、たとえば、インテル社より提供されている P I I X 4 というデバイスを選択することができる。IDE インタフェースには、IDE ハードディスク・ドライブ (HDD) 31 が接続される他、IDE CD-ROM ドライブ 32 が接続される。また、IDE CD-ROM 32 ドライブの代わりに、DVD (Digital Video Disc 又は Digital Versatile Disc) ドライブのような他のタイプの IDE 装置が接続されていても良い。HDD 31 や CD-ROM ドライブ 32 のような外部記憶装置は、例えばシステム 10 本体内の「メディア・ベイ」又は「デバイス・ベイ」と呼

ばれる収容場所に格納される。これら標準装備された外部記憶装置は、FDDやバッテリー・パックのような他の機器類と交換可能かつ排他的に取り付けられる場合もある。

【0026】

多機能PCIデバイス27にはRFIDタグとしての機能を発揮するRFIDチップ33が接続される。RFIDチップ33にはRFアンテナ37が接続される。RFアンテナ37は、HDD31をコンピュータ10に収納するためのデバイス・ベイの蓋部に組み込まれている。セキュリティ機能を必要としないユーザは、RFアンテナ37が組み込まれていないデバイス・ベイの蓋を選択することができる。すなわち、セキュリティ装置の一部としてのRFアンテナ37はオプション部品であり、ユーザ自らまたは販売店がアンテナ付き蓋またはアンテナ無し蓋のいずれか一方を装着することができる。RFIDチップ33は、リーダ／ライタが発信したRF励振信号をRFアンテナ37で受信して処理し、コンピュータの不正な持ち出しや不正なアクセスを禁止するセキュリティ機能を備えている。これらの要素はコンピュータ10のセキュリティ機能の一部を分担しており、後に動作の概要を説明する

【0027】

I/Oバス39としては、例えばISAバスがあり、Super I/Oコントローラ41、電源コントローラ45、FLASH ROM49等が接続される。Super I/Oコントローラ41は、フロッピー・ディスク・ドライブ(FDD)の駆動、パラレル・ポートを介したパラレル・データの入出力(PIO)、シリアル・ポートを介したシリアル・データの入出力(SIO)を制御するための周辺コントローラで、I/Oポート43が接続される。電源コントローラ45は主としてシステム内のパワー・マネジメントやサーマル・マネジメントを行うシングル・チップ・マイコンで、日立製作所から提供されるH8/300チップを選定することができる。電源コントローラ45は、MPU、RAM、ROMおよびタイマ等を備え、ROMにはパワー・マネジメントやサーマル・マネジメントを実行するのに必要なプログラムおよび参照テーブルを格納している。電源コントローラ45には、パワー・サプライ・コントローラ47が接続されてい

る。パワー・サプライ・コントローラ 47 にはバッテリーを充電するための充電器およびコンピュータ 10 で使用する 5V、3.3V 等の一定電圧を生成するための DC/DC コンバータが含まれ、電源コントローラ 45 のもとで直接的に電力制御を行う。

【0028】

FLASH ROM 49 は、キーボードやフロッピー・ディスク・ドライブ (FDD) などの各ハードウェアの入出力操作を制御するためのコード群 (BIOS: Basic Input/Output System) や、電源投入時の自己診断テスト・プログラム (POST: Power On Self Test) などのファームウェアを恒久的に格納するための書き換え可能な不揮発性メモリである。尚、コンピュータ・システム 10 を構成するためには、図 1 に示した以外にも多くの電気回路等が必要である。但し、これらは当業者には周知であり、また、本発明の要旨を構成するものではないので、本明細書中では省略している。

【0029】 [RFID を利用したセキュリティ機能]

RFID とは一般に RF (Radio frequency) すなわち無線を使って何らかの情報 ID (identification) を EEPROM に読み書きする機能であるということが出来る。RFID は単に無線を使った情報交換にとどまらず、一方にリーダー/ライタを配置し他方に RFID タグを配置した場合に両者間で情報交換するために RFID タグが電源を必要としないところに最大の特徴がある。リーダー/ライタは RFID タグに RF 励振信号を送り、RFID タグを励振して電力を発生させてデータを書き込みまたその電力を利用して RFID タグがデータをリーダー/ライタに送り返す。このような RFID によるデータの読み書き機能を利用して、電源が停止したコンピュータとリーダー・ライタとの間で多くの情報を交換することができコンピュータの在庫管理等に利用できる。

【0030】

RFID の他の利用形態としてコンピュータのセキュリティ機能に関するものがある。図 2 は、RFID タグとしての RFID チップ 33 の内部構成を概略的に記載したものである。このような RFID チップとしては、ATMEL 社から提供される AT24RF08 という型式の EEPROM (Asset Identification

EEPROM) がある。RFIDチップ33に含まれるEEPROM55は、記憶領域が8Kビットの一般エリア57と256ビットの特殊エリア59に分割されている。一般エリア57には、RFアンテナ37で受信したRF励振信号のデータがアナログ・インターフェース53を経由して書き込まれ、また書き込まれているデータはインターフェース53およびRFアンテナ37を経由して発信される。またEEPROM55とコンピュータ10はシリアル・インターフェース61およびSMB35を通じて通信し、コンピュータから一般エリア27および特殊エリア59への書き込みおよび読み出しができる。さらに、一般エリア57には本発明の実施例として二つの記憶領域が設けられている。一つは、RFアンテナの装着状況の履歴を示すAntenna Historyビットで、コンピュータ10へRFアンテナが装着されたことが検出されると「1」にセットされる。もう一つは、Antenna Errorビットで、一旦装着されたRFアンテナ37が脱着されたことが検出されると「1」にセットされる。Antenna HistoryビットおよびAntenna Errorビットは適切なパスワードを保有するユーザがSMB35およびシリアル・インターフェース61を経由してコンピュータ・システムからEEPROM55にアクセスしない限りリセットできない。

【0031】

特殊エリア59には、RFアンテナ37のコンピュータ10に対する着脱状態を検出するためのDE/DCビット領域、RFアンテナ37が監視区域のゲート近くに設置されたリーダ/ライタからRF励振信号を受信したときにセットするTamperビット領域、一般エリア57へのリード、ライトをロックするAccess Protectionビット領域、およびコンピュータの電源がオフになるまでAccess Protectionビットの変更をロックするStickyビット等が含まれる。Access Protectionビットは2ビットで構成され、「00または01」のときは一般エリアへの一切のアクセスが禁止され、「10」のときは読み出しだけが許可され、「11」のときは書き込みおよび読み出しが許可される。

【0032】

DE/DCビット領域は、DEビット (Detect Enable bit) とDCビット (Detect Coil bit) からなる。RFIDチップ33は、シリアル・インターフェース61を通じてDEビットが「1」にセットされるとRFアンテナ37の着脱状態をチェックし、RFアンテナ37が装着されているときは「1」を、脱着されているときは「0」をDCビットに書き込むようになっている。コンピュータの電源が入っている場合は電源部51がアナログ・インターフェース53を駆動するが、電源がない場合はRFアンテナ37を通じて受信したRF励振信号がアナログ・インターフェース53を駆動し、電源がない状態でもリーダ/ライタと通信できる。

【0033】 [本発明の実施例を適用するセキュリティ機能の概要]

次に本発明の実施例を適用するコンピュータのセキュリティ機能の概要を説明する。電源がオフになっているコンピュータが監視区域のゲートに近づくと、リーダ/ライタが発信するRF励振信号がRFアンテナ37に送られ、EEPROM55の特殊エリア59にTamperビットがセットされる。つぎにコンピュータの電源を投入すると、FLASH ROM49に格納されているBIOSがメイン・メモリ17に書き込まれ、CPU11はPOSTおよびシステムの初期化を実行する。POSTがTamperビットを検出するとパスワードの入力をユーザに要求すると共にその時点でPOSTの実行を停止し、パスワードの入力がない限りコンピュータへアクセスすることはできなくなる。

【0034】

前述のようにRFアンテナ37はユーザまたは販売店が装着できるようにしているため、不正にコンピュータを外に持ち出そうとする者がRFアンテナ37を外してからゲートを通過し、Tamperビットがセットされるのを回避しようとする可能性がある。本発明の実施例では、RFアンテナ37はオプションとして取り付けるが、その他のハードウェアはRFアンテナ37を装着する場合と脱着する場合とで共通である。また、RFアンテナ37を装着する場合とRFアンテナを脱着する場合のいずれにおいても同一のソフトウェア (BIOS) を採用できる。以下において、RFアンテナ37が不正に脱着された場合にコンピュータへのアクセスを禁止するための手順の実施例を説明する。

【0035】 [本発明の手順を示す第一の実施例]

図3は本発明の手順を示す第一の実施例としてのフローチャートである。コンピュータ10にRFアンテナが実際に装着されてセキュリティ機能が有効になるか否かは、この時点でシステムにとって不明である。コンピュータ10のAntenna HistoryビットおよびAntenna Errorビットは、工場から出荷する時点では共に「0」にセットされている。ブロック101でコンピュータ10の電源をオンにすると、BIOSがFLASH ROM49からメイン・メモリ17に読み出され、CPU11がPOSTプログラムを読みとって以下の手順を実行する。RFIDチップ33は、電源投入時点では常にAccess Protectionビットが「11」にStickyビットが「1」にセットされ、一般エリア57へのBIOSによるアクセスが許可される。ブロック103でPOSTは現実にはRFアンテナ37がコンピュータに装着されているか否かを確認するために特殊エリア59のDEビットを「1」にセットする。これに応じてRFIDチップ33はRFアンテナ37の装着状態をチェックし、装着されていればDCビットに「1」を脱着されていれば「0」を書き込む。

【0036】

POSTはDEビットを「1」にセットしてから約200マイクロ秒経過した後DCビットを読みとり、さらにDEビットを「0」にセットする。DCビットが「1」にセットされて現在RFアンテナ37が装着されていることが確認されたならばブロック105に移行して一般エリア57のAntenna Historyビットを「1」にセットする。この時点で、コンピュータ10がセキュリティ機能を具備するコンピュータであることがシステムによって認識されたことになり、以後Antenna Historyビットは、パスワードを有するユーザが書き換ええない限り電源がオフになってもこの情報を維持し続ける。DCビットが「0」でRFアンテナが脱着されていることが確認されたならば、ブロック107に移行して一般エリア57のAntenna Errorビットを確認する。Antenna Errorビットをこの時点で確認することは、後にブロック109で詳細に説明するが、前回のPOSTを実行する以前に一旦装着されたRFアンテナが脱着されたことがあったか否かを確認することに相当する。

【0037】

ブロック107でAntenna Errorビットが「1」のときは、前回のPOSTを実行する以前にRFアンテナ37が一旦装着され、さらに前回のPOSTを実行する段階でRFアンテナ37が脱着されていた場合であり、RFアンテナの不正な脱着があったものとしてこれを処理するブロック119に移行する。以後Antenna Errorビットは、パスワードを有するユーザが書き換えられない限り電源がオフになってもこの情報を維持し続ける。ブロック107でAntenna Errorビットが「0」のときは、すくなくとも前回のPOSTの実行時点まではRFアンテナの不正な脱着がなかったものと判断し、ブロック111に移行する。

【0038】

ブロック111では、Antenna Historyビットを確認する。すなわち、今回のPOSTを実行する時点までにRFアンテナ37がコンピュータ10に装着されたことがあるか否かを確認する。Antenna Historyビットへのデータは、ブロック105により今回のPOST実行時に、または前回以前のPOST時に書き込まれる。ブロック111でAntenna Historyビットが「0」のときは、現在までRFアンテナが装着されたことがない場合であってコンピュータ10はセキュリティ機能を有しないコンピュータであることを意味しており、ブロック115に移行する。ブロック111でAntenna Historyビットが「1」のときは、今回のPOSTを実行する時点までにRFアンテナが装着されたことがあり、かつ前回のPOSTを実行する時点までの間に一旦装着されたRFアンテナが脱着されたことがPOSTで検出されていない場合（Antenna Errorビット=0）であり、ブロック113に移行する。

【0039】

ブロック113ではDCビットを再度確認し、今回のPOST実行時点でRFアンテナ37が装着されているか脱着されているかを判断する。DCビットが「1」すなわち現実にはRFアンテナ37がコンピュータ10に装着されていれば、セキュリティ装置の脱着はなかったものとしてブロック115に移行する。DC

ビットが「0」のときは、今回のPOSTを実行する以前にRFアンテナが装着されていたが（ブロック111）今回のPOSTを実行する段階では脱着されており（ブロック113）、さらに前回のPOSTを実行する以前に一旦装着されたRFアンテナが前回以前のPOSTを実行する段階で脱着されたことが検出されていない（ブロック107）場合であり、ブロック109に移行して処理される。言い換えると、これは前回のPOSTを実行してから今回のPOSTを実行するまでの間にRFアンテナが脱着された場合を今回のPOSTで処理する手順である。前回のPOSTを実行する時点においてそれまでに一旦装着されたRFアンテナ37が脱着されていると、前回のPOSTを実行する時点でAntenna Errorビットが「1」にセットされ、今回のPOSTを実行するとブロック107からブロック119に移行して処理されるからである。

【0040】

ブロック115は、ブロック111から移行する手順で示されるセキュリティ機能を有しないコンピュータと、ブロック113から移行する手順で示されるセキュリティ機能を有しかつRFアンテナ37が一旦装着された後に脱着されたことがないコンピュータとを処理する。この場合は、セキュリティ装置の脱着はないので、Access Protectionビットを「10」にセットし、以後一般エリアのAntenna HistoryビットおよびAntenna Errorビットへの書き込みを禁止する。さらにStickyビットを「0」にセットして、コンピュータの電源が切られるまでAccess Protectionビットの変更ができないようにする。これは、OS経由でAccess Protectionビットが「11」に変更され、Antenna HistoryビットまたはAntenna Errorビットの内容が書き換えられるのを防止するためである。この結果Antenna HistoryビットおよびAntenna Errorビットの書き換えは、電源がオンになったブロック101からブロック115までの間だけ可能になり、実際はこの間にPOSTだけがビットの書き換えをすることになる。続いてブロック117に移行し、BIOSはブートストラップを実行し、OSおよびアプリケーション・プログラムをメイン・メモリに読み出しコンピュータの構成を行う。

【0041】

ブロック109ではAntenna Errorビットを「1」に書き換える。Antenna ErrorビットはPOSTを実行する毎にブロック107ないしブロック113が判断され、その結果に応じて「1」に書き換えられる。ブロック109は、前回のPOSTを終了した時点ではAntenna Errorビットが「1」に書き換えられていなかったが（ブロック107）、今回のPOSTを実行した時点で過去においてRFアンテナ37が装着されたことがある（ブロック111）にも係わらず現在それが脱着されている（ブロック113）場合を処理する。

【0042】

続いてブロック109からブロック119に移行する。さらにブロック107で判断したAntenna Errorビットが「1」である場合もブロック119に移行する。ブロック119では今回のPOSTを実行する間にブロック109によりAntenna Errorビットが「1」にセットされた場合および前回のPOSTを終了するまでの間にAntenna Errorビットが「1」であったことに応答してコンピュータ10のディスプレイにPOSTエラーの表示をする。

【0043】

次にブロック121でディスプレイにユーザにパスワードを要求するメッセージを表示し、BIOSがブロック123で正しいパスワードの入力を認識すると、ブロック127でAntenna HistoryビットおよびAntenna Errorビットを「0」に書き換える。続いてブロック129でPOSTを再スタートする。再スタートしたPOSTでは、POSTエラーの表示ができることはなくブロック101からブロック117までの手順をクリアしてブートストラップが実行される。

【0044】

BIOSがブロック123で正しいパスワードを認識しないとその時点でPOSTは停止し、以後コンピュータへのアクセスはできなくなる。それ以降正しいパスワードを入力できる場合は、再度ブロック101の電源オンからスタートし

て、ブロック 121 で正しいパスワードを入力してからブロック 129 を経由して再度ブートストラップを実行する。

【0045】 [本発明の手順を示す第二の実施例]

図 3 のフローチャートで説明した手順では、電源がオンの状態で RF アンテナが不正に外されてコンピュータが外部に持ち出されても、一旦電源をオフにして POST を実行する段階にならないとコンピュータへのアクセスを禁止することはできない。電源オンの状態で RF アンテナが外されてしまうことに対処するために、本発明の手順を示す第二の実施例としてのフローチャートを図 4 に示す。電源が投入され、図 3 で説明した手順で POST が実行されてブースストラップが開始されると、デバイス・ドライバによってブロック 151 から始まる第二の実施例の手順が開始される。ブロック 153 では Antenna History ビットが確認される。今回の POST を実行する時に RF アンテナが装着されていれば図 3 のブロック 105 で Antenna History ビットは「1」にセットされている。ブロック 153 では、Antenna History ビットを確認し、ビットが「0」で RF アンテナが装着されていないければブロック 157 へ移行し本手順は終了する。

【0046】

ブロック 153 で確認したビットが「1」で今回の POST を実行した時点で RF アンテナが装着されていれば、ブロック 155 に移行する。ブロック 155 でポーリングにより定期的に DC ビットの状態を確認する。このポーリングは実際には他のプログラムの実行を妨げないように、タイマー・インターラプトなどによって行われることが好ましい。RF アンテナ 37 が脱着されない限り CPU は RF アンテナの装着状態を定期的に監視する。RF アンテナ 37 が脱着されるとブロック 159 に移行しコンピュータの電源が強制的にオフにされるので、ユーザが再度電源をオンにすると図 3 に示した POST が再スタートさせられる。図 3 の手順ではブロック 103、107、111、113、109、119、121 のルートに従って処理され、パスワードが要求される。すなわちコンピュータの電源オンの状態において、一旦装着された RF アンテナ 37 が脱着されると、CPU 11 のポーリングのタイミングでコンピュータの電源がオフにされるの

で、次回の電源をオンにしたときPOSTが実行され、パスワードを入力できないユーザはそれ以上コンピュータにアクセスできないことになる。

【0047】

以上本発明の手順をBIOSのPOSTで実行する場合を例にして説明してきたが、本発明を実行するプログラムはPOSTに限定されるものではなく、他のBIOS、デバイス・ドライバ、OS、またはアプリケーション・ソフトといわれる各種ソフトウェアを利用して実行することができる。POST以外のソフトウェアを利用する場合には、図3に示した手順を開始するタイミングとして、ユーザが特定のデータにアクセスした場合や、サスペンドまたはハイバーネーションといわれるような各種省エネ・モードに移行した場合等を採用することができる。

【0048】

図5に本発明を実行するコンピュータ10の外形の一例を示す。コンピュータ10は図1で説明した構成要素を収納する本体201、液晶ディスプレイ203、本体上部に配置したキーボード207、CD-ROMドライブ32、およびHDD31を収納するデバイス・ベイの蓋209を含む。コンピュータ10はデバイス・ベイの蓋209を除いて、本実施例との関連で特別な外形的特徴を備えるものではない。

【0049】

図6に本発明で使用するRFアンテナ37の装着方法の実施例を示す。RFアンテナ37はデバイス・ベイの蓋209に収納される。デバイス・ベイにHDD31が着脱可能な状態で装着した後に蓋209を本体201に対してはめ込み構造で取り付ける。RFアンテナ37を使用しない場合、すなわちセキュリティ機能を必要としないコンピュータでは、RFアンテナ37を取り付けずに蓋209だけを本体201に装着できる。また、蓋209とは異なりRFアンテナ37を収納できない構造の蓋を用意してもよい。このようなRFアンテナ37の取り付け構造を蓋209に採用することにより、ユーザまたは販売店でRFアンテナ37の取り付けが可能になり、ユーザはセキュリティ機能の必要性に応じてRFアンテナ37付きの蓋209またはRFアンテナ37なしの蓋209のいずれか

を選択できる。蓋 209 の内側には、アンテナ 37 用コイルが収納され、そのリード部 211 は蓋 209 の端子部にはめ込まれると共に、RFID チップ 33 に電氣的に接続される。

【0050】

このような方法で RF アンテナ 37 を取り付ける場所としては、HDD 用のデバイス・ベイの蓋部にとどまらず CD-ROM ドライブ、DVD ドライブ、FD D、バッテリ等の外部装置のデバイス・ベイの蓋や、これらを択一的に収納できるマルチ・ベイの蓋を利用できる。RF アンテナ 37 の本体 201 に対する取り付け構造は、コンピュータの使用場所において不正行為者が短時間に脱着できるものではなく、かつ販売店またはユーザがある程度の時間を費やして着脱できる程度に強固なものであることが好ましい。たとえば、はめ込み構造に加えてスクリューで締め付ける構造や、そのスクリューに特殊な工具を要するものを採用することができる。

【0051】

本発明の実施例は RFID を利用したセキュリティ装置の脱着が行われたときにコンピュータへのアクセスを禁止する例で説明したが、本発明の適用範囲は RFID に限定されるものではなく、たとえば指紋によりコンピュータへのアクセス資格を確認するような他の種類のセキュリティ装置にも適用できる。

【0052】

【発明の効果】

本発明により、セキュリティ装置が不正に脱着されたときにアクセスができなくなるコンピュータを提供することができた。さらに本発明によりセキュリティ機能の有無だけが相違するコンピュータにおいて、セキュリティ装置以外はハードウェアおよびソフトウェアが共通なコンピュータを提供することができた。また本発明により、装着および脱着が可能で余分なスペースを必要としないセキュリティ装置の取り付け構造を備えたコンピュータを提供することができた。

【図面の簡単な説明】

【符号の説明】

【図 1】 本発明を実施するコンピュータの概略ブロック図の一例である。

【図 2】 本発明の実施例で使用する R F I Dチップの概略ブロック図である。

【図 3】 本発明の手順を示す第一の実施例のフローチャートである。

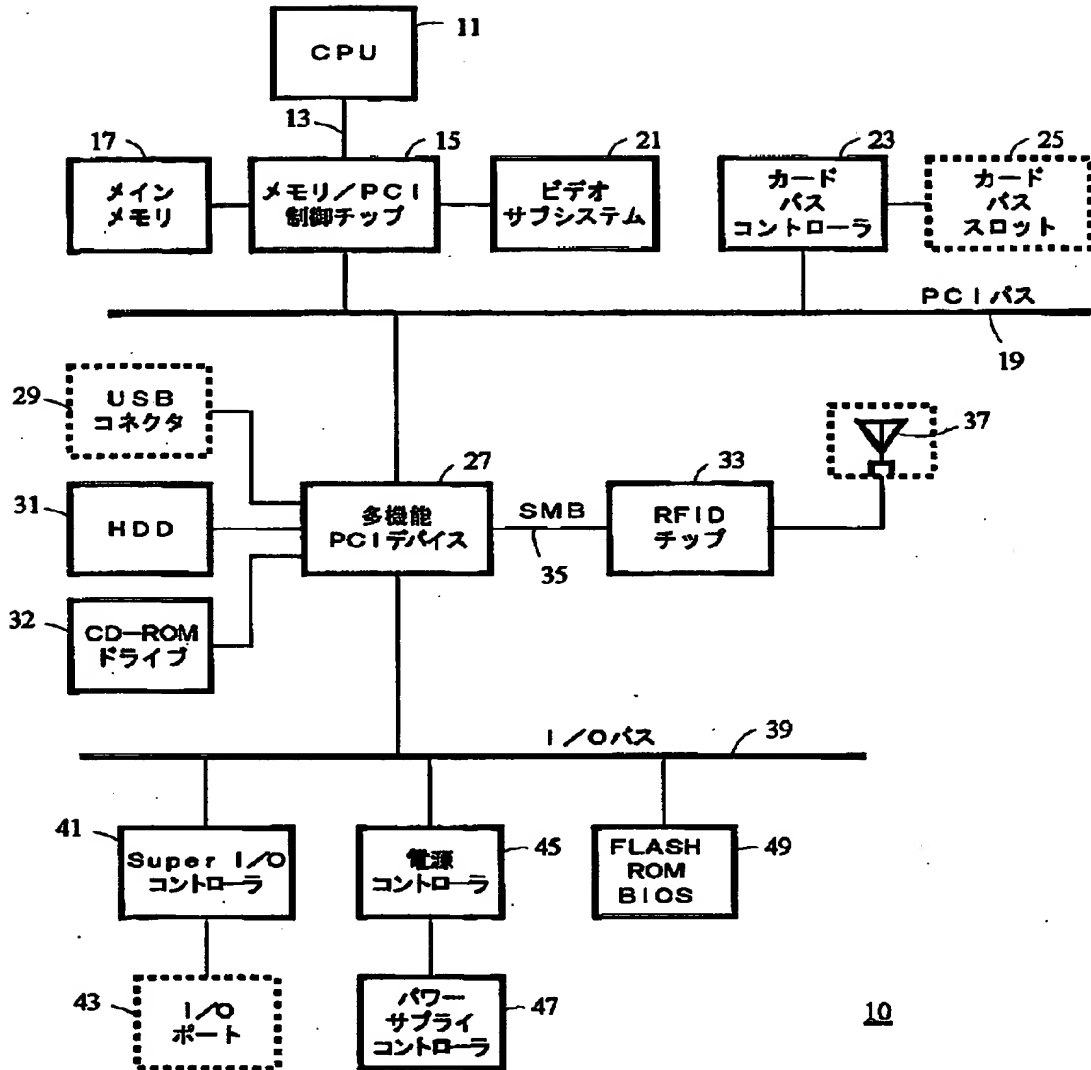
【図 4】 本発明の手順を示す第二の実施例のフローチャートである。

【図 5】 本発明を実施するコンピュータの外形図の一例である。

【図 6】 本発明の実施例で使用する R F アンテナの取り付け方法の一例を示す図である。

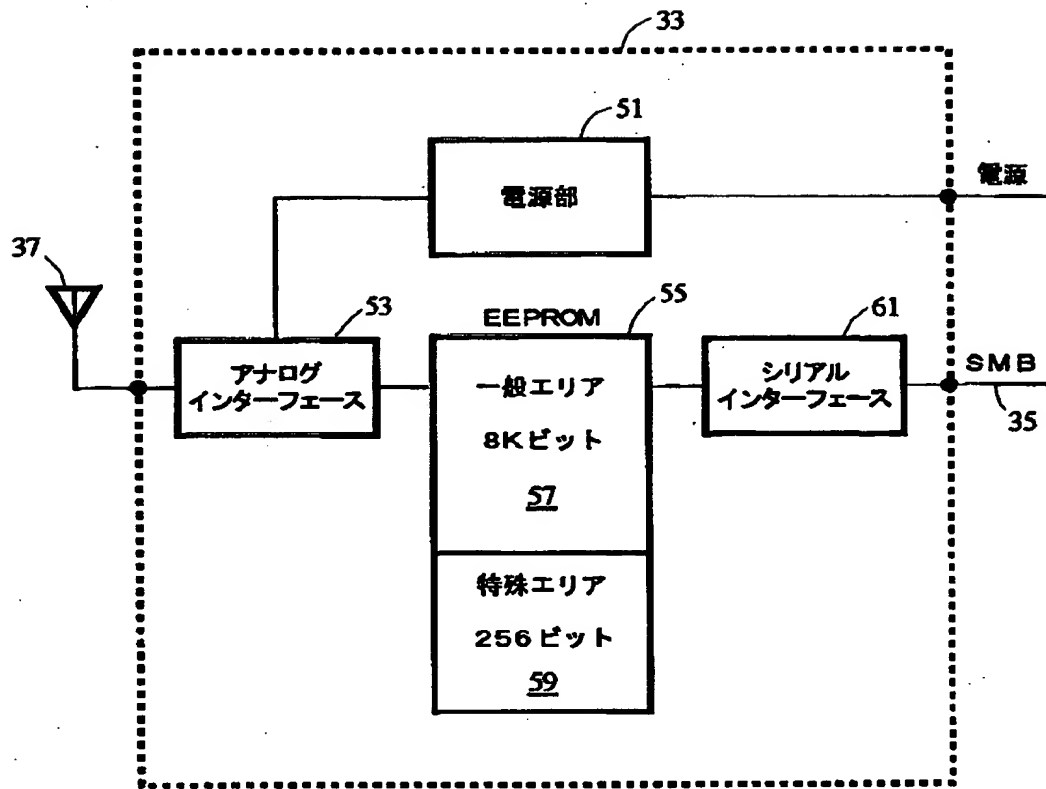
【書類名】 図面

【図 1】

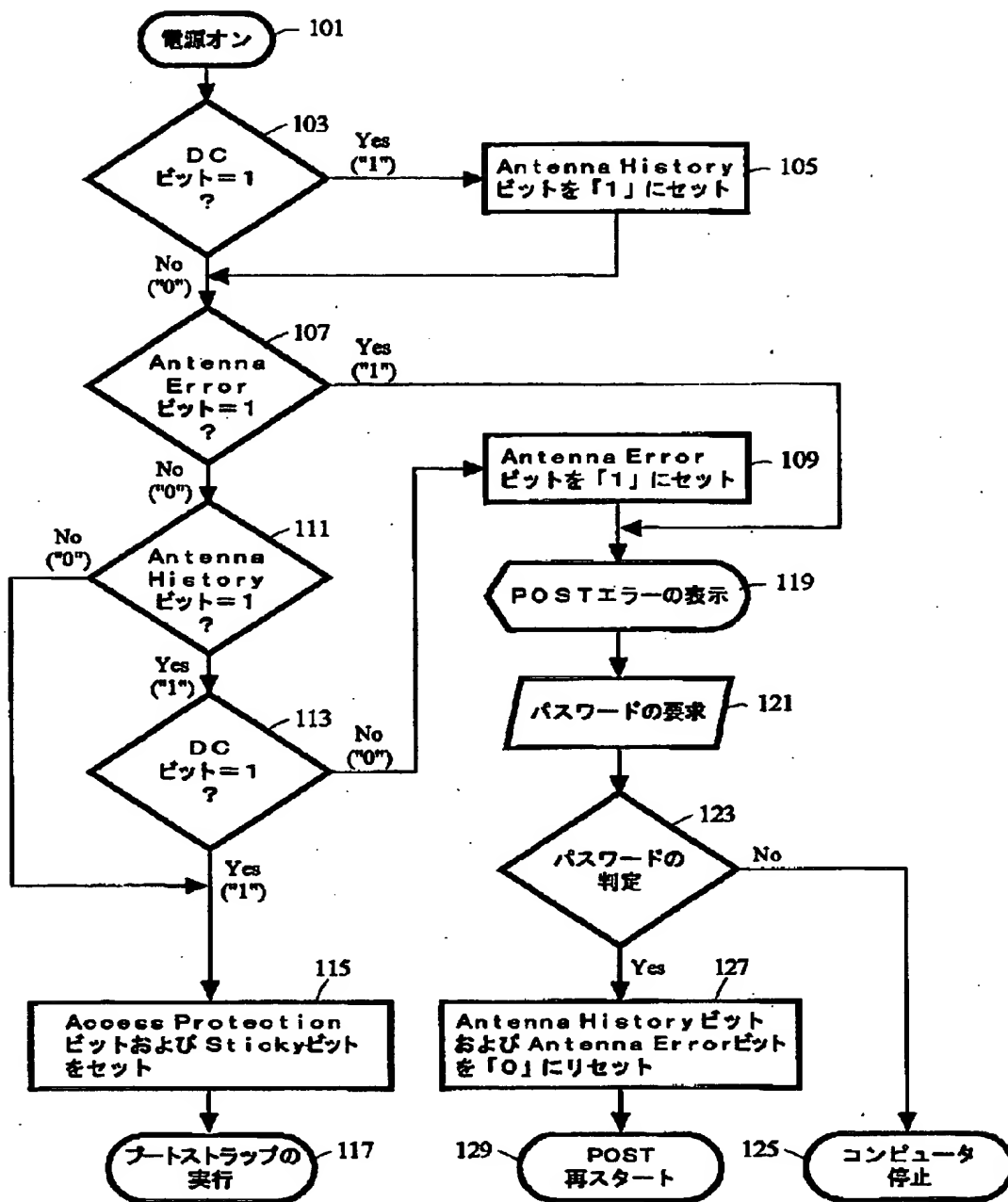


10

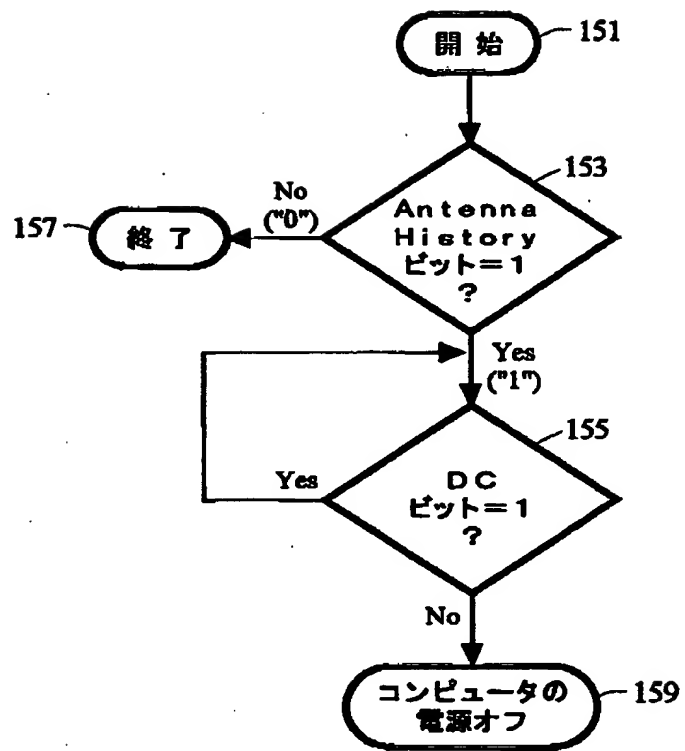
【図 2】



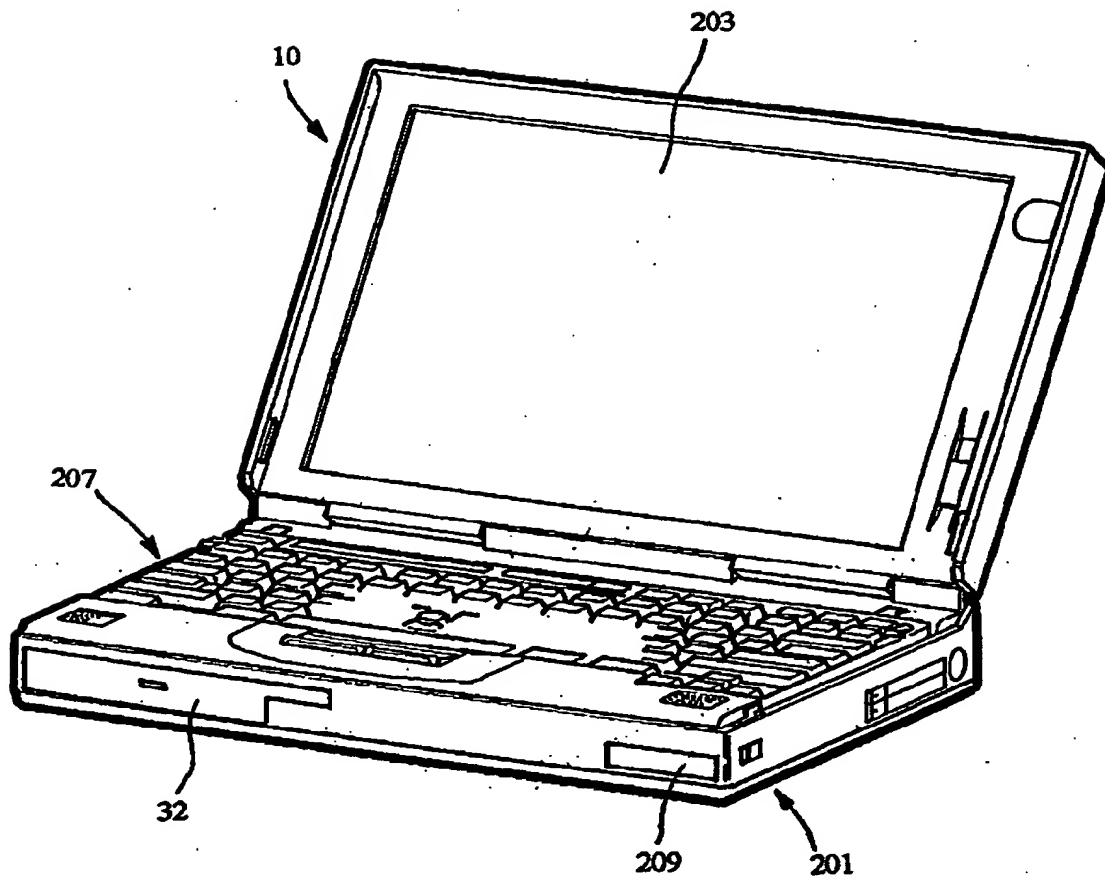
【図 3】



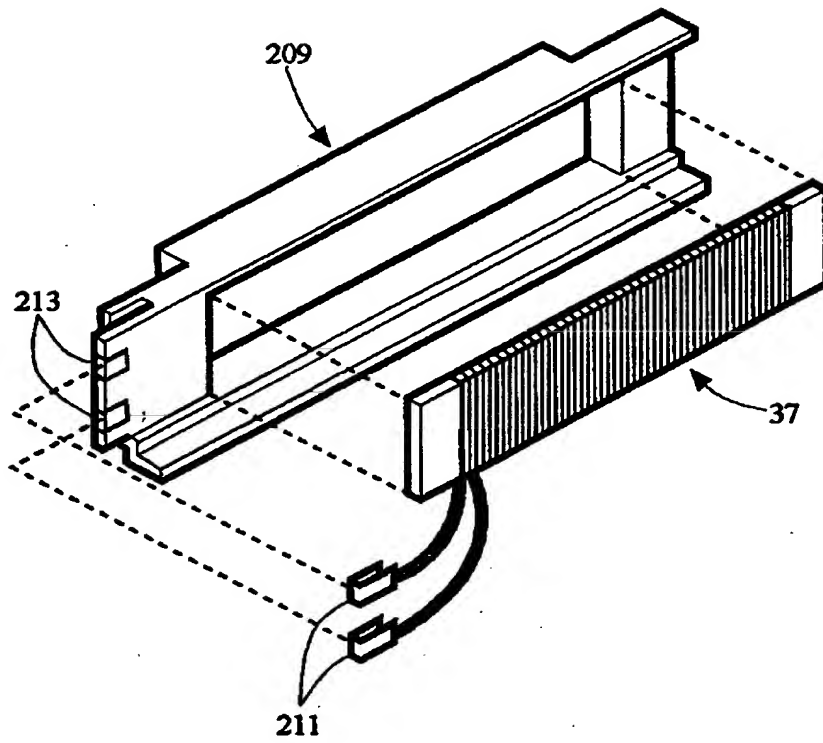
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 セキュリティ機能付きコンピュータのセキュリティ装置が不正に取り外された場合にコンピュータへのアクセスを禁止する技術を提供する。

【解決手段】 セキュリティ装置はコンピュータのセキュリティ機能の一部を担うハードウェアであり、不正に脱着された場合に以下の手順でアクセスを禁止する。コンピュータにセキュリティ装置が装着されたこと示すデータを不揮発性メモリに記憶し保持する。そのあとに電源オン等の何らかのイベントをきっかけとしてコンピュータへのアクセスを禁止する手順を開始する。続いてメモリのデータに基づいてセキュリティ装置が装着されたことがあることを検出する。さらにコンピュータから現在セキュリティ装置が脱着されていることを検出する。セキュリティ装置が装着されたことがあるにも係わらず現在脱着されているならば、コンピュータへのアクセスを禁止する。

【選択図】 図3

認定・付加情報

特許出願の番号	平成11年 特許願 第013215号
受付番号	59900049410
書類名	特許願
担当官	第二担当上席 0091
作成日	平成11年 1月25日

<認定情報・付加情報>

【提出日】	平成11年 1月21日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [390009531]

1. 変更年月日 1990年10月24日

[変更理由] 新規登録

住 所 アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)

氏 名 インターナショナル・ビジネス・マシーンズ・コーポレイション